1-29-1999

Some Recent Developments in Difference Sets

James A. Davis
University of Richmond, jdavis@richmond.edu

Jonathan Jedwab

JAMES A DAVIS and JONATHAN JEDWAB

Some recent developments in difference sets

1 Introduction

A k-element subset D of a finite multiplicative group G of order v is called a (v, k, λ, n)-*difference set in* G provided that the multiset of "differences" given by $\{d_1 d_2^{-1} \mid d_1, d_2 \in D, d_1 \neq d_2\}$ contains each nonidentity element of G exactly λ times; we write $n = k - \lambda$. For example, $D = \{x, x^2, x^4\}$ is a $(7, 3, 1, 2)$-difference set in $\mathbb{Z}_7 = \langle x \mid x^7 = 1 \rangle$.

There are five known parameter families for (v, k, λ, n)-difference sets satisfying the condition $\gcd(v, n) > 1$: the *Hadamard, McFarland, Spence, Davis-Jedwab,* and *Chen* families. The present authors recently gave a recursive unifying construction for difference sets from the first four families which relies on relative difference sets. This paper gives an overview of this construction and shows that, by modifying it to use *divisible* difference sets in place of *relative* difference sets, the recent difference set discoveries of Chen can be brought within the unifying framework. It also demonstrates the recursive use of an auxiliary construction for divisible difference sets by means of an extended example.

Difference sets arise in a wide variety of theoretical and applied contexts. They are important in design theory because a (v, k, λ, n)-difference set in G is equivalent to a symmetric (v, k, λ, n)-design with a regular automorphism group G [15]. The study of difference sets is also deeply connected with coding theory because the code, over a field F, of the symmetric design corresponding to a (v, k, λ, n)-difference set may be considered as the right ideal generated by D in the group algebra FG [12], [15]. Difference sets in abelian groups are the natural solution to many problems of signal design in digital communications [7]. For a recent survey of difference sets see the paper by Jungnickel [12] and its update by Jungnickel and Schmidt [13], or see the difference sets chapter of Beth, Jungnickel and Lenz [3].

The central problem is to determine, for each parameter set (v, k, λ, n), which groups of order v contain a difference set with these parameters. An extensive literature has been devoted to this problem, exposing considerable interplay between difference sets and such diverse branches of mathematics as algebraic number theory, character theory, representation theory, finite geometry and graph theory. Nonetheless the central problem remains open, both for abelian and nonabelian groups, except for heavily restricted parameter sets. One of the most popular techniques for constructing a difference set or for ruling out its existence is to consider the image of a hypothetical difference set under mappings from the group G to one or more quotient groups G/U (see Ma and Schmidt [18] for a recent example).

By a counting argument the parameters (v, k, λ, n) of a difference set are related by $k(k-1) = \lambda(v-1)$. The trivial cases $k = 0$ and $k = 1$ are usually excluded

(although trivial examples are used as the initial case of some recursive constructions in [7]). Besides this constraint, difference sets are classified into families according to further relationships between the parameters. Jungnickel and Schmidt [13] group the known families into three classes according to their methods of construction:

Singer difference sets. This class comprises the classical Singer family (known alternatively as the Projective Geometries family) and the Gordon-Mills-Welch family. The difference sets in this class occur in cyclic groups, and are obtained from the action of a cyclic group of linear transformations on the one-dimensional subspaces of a finite field.

Cyclotomic difference sets. This class comprises the Paley family, the families involving residues of higher order than quadratic, and the Twin Prime Power family. The difference sets in this class occur in elementary abelian groups, or the product of two such groups, and are unions of cosets of multiplicative subgroups of a finite field.

Difference sets with $\gcd(v, n) > 1$. This class comprises all the remaining five known families of difference sets, namely Hadamard, McFarland, Spence, Davis-Jedwab, and Chen. This class has attracted a great deal of research interest, and is the subject of the rest of this paper.

The Hadamard family is given by

$$(v, k, \lambda, n) = (4N^2,\ N(2N-1),\ N(N-1),\ N^2) \tag{1.1}$$

for integer $N \geq 1$ (see Davis and Jedwab [8] for a survey, and Jungnickel and Schmidt [13] for an update). The Hadamard family derives its name from the fact that D is a Hadamard difference set if and only if the $(+1, -1)$ incidence matrix of the design corresponding to D is a regular Hadamard matrix [12], [22].

The McFarland family is given by

$$(v, k, \lambda, n) = \left(q^{d+1}\left(\frac{q^{d+1}-1}{q-1}+1\right),\ q^d\left(\frac{q^{d+1}-1}{q-1}\right),\ q^d\left(\frac{q^d-1}{q-1}\right),\ q^{2d}\right) \tag{1.2}$$

for q a prime power and integer $d \geq 0$ (see Ma and Schmidt [17] for a summary and new results). The Hadamard and McFarland families intersect in 2-groups: the Hadamard family with $N = 2^d$ corresponds to the McFarland family with $q = 2$.

The Spence family is given by

$$(v, k, \lambda, n) = \left(3^{d+1}\left(\frac{3^{d+1}-1}{2}\right),\ 3^d\left(\frac{3^{d+1}+1}{2}\right),\ 3^d\left(\frac{3^d+1}{2}\right),\ 3^{2d}\right) \tag{1.3}$$

for integer $d \geq 0$.

The Davis-Jedwab family, introduced in [7] and named in [3], is given by

$$(v,k,\lambda,n) = \left(2^{2d+4}\left(\frac{2^{2d+2}-1}{3}\right), 2^{2d+1}\left(\frac{2^{2d+3}+1}{3}\right), 2^{2d+1}\left(\frac{2^{2d+1}+1}{3}\right), 2^{4d+2}\right) \tag{1.4}$$

for integer $d \geq 0$.

The Chen family, introduced in [4], [5] and named in [3], is given by $(v,k,\lambda,n) =$

$$\left(4q^{2d+2}\left(\frac{q^{2d+2}-1}{q^2-1}\right), q^{2d+1}\left(\frac{2(q^{2d+2}-1)}{q+1}+1\right), q^{2d+1}(q-1)\left(\frac{q^{2d+1}+1}{q+1}\right), q^{4d+2}\right) \tag{1.5}$$

for integer $d \geq 0$ and q a prime power.

The Chen family with $d = 0$ corresponds to the Hadamard family with $N = q$; the Chen family with $q = 2$ corresponds to the Davis-Jedwab family; and the Chen family with $q = 3$ corresponds to the Spence family with d replaced by $2d+1$. The Davis-Jedwab and Chen families are the first new families of difference sets to be discovered since 1977. (We have followed [3] in naming these two families separately because the known constructions for the family (1.4) deal with more general groups than the known constructions for the family (1.5) when applied to the case $q = 2$.)

For each of these parameter families, the existence question has been solved for infinitely many values of the parameters, but not necessarily for all possible groups of a given order. The following two results, which give complete solutions to the central problem for certain classes of difference set, are notable exceptions. (The *exponent* of a group G with identity 1_G, written $\exp(G)$, is the smallest integer α for which $g^\alpha = 1_G$ for all $g \in G$.)

Theorem 1.1 *A Hadamard difference set exists in an abelian group G of order 2^{2d+2} if and only if $\exp(G) \leq 2^{d+2}$.*

Theorem 1.2 *A McFarland difference set with $q = 4$ exists in an abelian group G of order $2^{2d+3}(2^{2d+1}+1)/3$ if and only if the Sylow 2-subgroup of G has exponent at most 4.*

The constructive part of Theorem 1.1 is due to Kraemer [14] and the nonexistence part is due to Turyn [22]. The constructive part of Theorem 1.2 is due to Davis and Jedwab [7] and the nonexistence part is due to Ma and Schmidt [16].

The present authors showed in [7] that the Hadamard, McFarland, Spence and Davis-Jedwab parameter families can be unified by means of a recursive construction which depends on the existence of certain relative difference sets. The required relative difference sets are themselves constructed by means of a second recursive construction. This method deals with all abelian groups known to contain such difference sets (although certain initial examples required for the Hadamard family must be constructed separately). In this paper we show that by modifying these two recursive constructions to use divisible difference sets in place of relative difference

sets, we can bring the recent constructions [4], [5] of Chen difference sets within the unifying framework, reinforcing Jungnickel and Schmidt's grouping [13] of difference set parameter families into the three classes mentioned above. We believe this viewpoint may assist the construction of Chen difference sets in new groups, although we emphasise that in terms of elegance and directness we prefer Chen's original constructions.

A k-element subset R of a finite multiplicative group G of order mu containing a normal subgroup U of order u is called a $(m, u, k, \lambda_1, \lambda_2)$ *divisible difference set (DDS) in G relative to U* provided that the multiset $\{r_1 r_2^{-1} \mid r_1, r_2 \in R, r_1 \neq r_2\}$ contains each nonidentity element of U exactly λ_1 times and each element of $G \setminus U$ exactly λ_2 times. For example, $R = \{1, x, y, xy, xy^2, x^2y^2\}$ is a $(3, 3, 6, 3, 4)$ DDS in the group $\mathbb{Z}_3^2 = \langle x, y \mid x^3 = y^3 = 1\rangle$ relative to $\langle x\rangle \cong \mathbb{Z}_3$. A $(m, u, k, \lambda_1, \lambda_2)$ DDS in G, relative to some normal subgroup U, is equivalent to a square divisible $(m, u, k, \lambda_1, \lambda_2)$-design whose automorphism group G acts regularly on points and blocks [11]. For a recent overview of DDSs, see Pott [19]. The central problem is to determine, for each parameter set $(m, u, k, \lambda_1, \lambda_2)$, the groups G of order mu and the normal subgroups U of order u for which G contains a DDS relative to U with these parameters. However, the definition of DDS is so general that the central problem is usually of interest only when its solution throws light on another combinatorial problem, or when the parameters are further constrained.

In the important special case $\lambda_1 = 0$, a divisible difference set is called a *relative difference set* (RDS), the parameter list is abbreviated to (m, u, k, λ_2), and the subgroup U is called the *forbidden* subgroup. The set $R = \{1, x, y, xy^3, z, xy^2z, x^2y^3z, x^3y^3z\}$ is an example of a $(8, 4, 8, 2)$ RDS in $\mathbb{Z}_4^2 \times \mathbb{Z}_2 = \langle x, y, z \mid x^4 = y^4 = z^2 = 1\rangle$ relative to $\langle x^2, y^2\rangle \cong \mathbb{Z}_2^2$. See Pott [20] for a recent survey of RDSs, and [7], [9] for new constructions. In the special case $\lambda_1 = \lambda_2$, a divisible difference set is equivalent to a $(mu, k, \lambda_2, k - \lambda_2)$-difference set in G.

By a counting argument, the parameters $(m, u, k, \lambda_1, \lambda_2)$ of a DDS are related by $k(k-1) = \lambda_1(u-1) + \lambda_2 u(m-1)$. If $k^2 - \lambda_2 um = 0$ (which by the counting relationship is equivalent to $k - \lambda_1 + u(\lambda_1 - \lambda_2) = 0$) then the DDS is called *semi-regular*. In the special case of a RDS, the parameters are semi-regular if $k - u\lambda_2 = 0$, and the RDS parameters can then be written in the form $(u\lambda_2, u, u\lambda_2, \lambda_2)$. Pott [19] suggests that semi-regular divisible difference sets merit careful study, noting that the special case of semi-regular relative difference sets is of particular interest. Indeed, the RDSs required in the recursive constructions of [7] have semi-regular parameters, and the generalisation to DDSs of this paper also requires semi-regular parameters.

Difference sets are usually studied in the context of the group ring $\mathbb{Z}[G]$ of the group G over the ring of integers $\mathbb{Z}$. The definition of a (v, k, λ, n)-difference set D in G is equivalent to the equation $DD^{(-1)} = n1_G + \lambda G$ in $\mathbb{Z}[G]$, where by an abuse of notation we have identified the sets $D, D^{(-1)}, G$ with the respective group ring elements $D = \sum_{d\in D} d$, $D^{(-1)} = \sum_{d\in D} d^{-1}$, $G = \sum_{g\in G} g$, and 1_G is the identity of G. Similarly the definition of a $(m, u, k, \lambda_1, \lambda_2)$ DDS R in G relative to U is equivalent to the equation $RR^{(-1)} = k1_G + \lambda_1(U - 1_G) + \lambda_2(G - U)$ in $\mathbb{Z}[G]$. We shall follow the

practice (standard in the difference set literature) of abusing notation by identifying sets with group ring elements, as in the examples above.

In the remainder of this paper, all groups mentioned should be understood to be abelian even if this is not explicitly stated.

We shall require the following definitions and results. A *character* of a group G is a homomorphism from G to the multiplicative group of complex roots of unity. Under pointwise multiplication the set G^* of characters of G forms a group isomorphic to G. The identity of this group is the *principal character* that maps every element of G to 1. The *character sum* of a character χ over the group ring element C corresponding to a subset of G is $\chi(C) = \sum_{c \in C} \chi(c)$. It is well known (see [19], for example) that the character sum $\chi(C)$ is 0 for all non-principal characters χ of G if and only if C is a multiple of G (regarded as a group ring element). If a character χ is non-principal on G and principal on a subgroup U then χ induces a non-principal character ψ on G/U defined by $\psi(gU) = \chi(g)$.

The use of character sums to study difference sets was introduced by Turyn in his seminal paper [22] and subsequently extended to relative difference sets and divisible difference sets:

Lemma 1.3

(i) The k-element subset D of a group G of order v is a (v, k, λ, n)-difference set in G if and only if $|\chi(D)| = \sqrt{n}$ for every non-principal character χ of G.

(ii) The k-element subset R of a group G of order mu containing a subgroup U of order u is a (m, u, k, λ) RDS in G relative to U if and only if for every non-principal character χ of G:

$$|\chi(R)| = \begin{cases} \sqrt{k} & \text{if } \chi \text{ is non-principal on } U; \\ \sqrt{k - u\lambda} & \text{if } \chi \text{ is principal on } U. \end{cases}$$

(iii) The k-element subset R of a group G of order mu containing a subgroup U of order u is a $(m, u, k, \lambda_1, \lambda_2)$ DDS in G relative to U if and only if for every non-principal character χ of G:

$$|\chi(R)| = \begin{cases} \sqrt{k - \lambda_1} & \text{if } \chi \text{ is non-principal on } U; \\ \sqrt{k - \lambda_1 + u(\lambda_1 - \lambda_2)} & \text{if } \chi \text{ is principal on } U. \end{cases}$$

Parts (i) and (ii) of Lemma 1.3 can be regarded as special cases of part (iii). Lemma 1.3 indicates a general strategy for constructing difference sets, relative difference sets and divisible difference sets, namely to choose a group subset for which all non-principal character sums have the correct modulus. In [7] the authors showed that the determination of character sums can be greatly facilitated by selecting the group subset to be the union of cosets of "building blocks" whose character properties interact in a simple way. By Lemma 1.3 (ii), a semi-regular RDS in G relative to U

has the key property that, for any non-principal character χ of G, the character sum has fixed modulus when χ is non-principal on U and is zero when χ is principal on U. By Lemma 1.3 (iii) the same property holds for a semi-regular divisible difference set in G relative to U. We shall show that this allows the recursive constructions of [7] to be naturally generalised to use divisible difference sets in place of relative difference sets. Although several of the generalisations require only minor modification of the constructions of [7], for completeness we shall give full proofs.

2 Constructions

Following [7], we introduce two definitions:

Definition *A building block in a group G with modulus m* is a subset of G such that all non-principal character sums over the subset have modulus either 0 or m.

Definition For integers $a \geq 1$ and $t \geq 1$, *a (a, m, t) building set (BS) on a group G relative to a subgroup U* is a collection of t building blocks in G with modulus m, each containing a elements, such that for every non-principal character χ of G:

(i) exactly one building block has nonzero character sum if χ is non-principal on U;

(ii) each building block has zero character sum if χ is principal on U.

Following [3], we call the BS *covering* in the case $U = G$, when exactly one building block has nonzero character sum for every non-principal character of G. (The use of "covering" refers not to the intersection or union of the building blocks but to their character properties.)

The (a, m, t) BSs studied in [7] satisfy the constraint $m = \sqrt{at}$ and give rise to semi-regular RDSs. By removing this constraint we obtain semi-regular DDSs. We begin by considering the case $t = 1$.

Lemma 2.1 *Suppose B is a $(a, m, 1)$ BS on a group G relative to a subgroup $U \neq G$ of order u. Then B is a $(a^2/(u(a-m^2)+m^2), u, a, a-m^2, a-m^2+m^2/u)$ semi-regular DDS in G relative to U.*

Proof It follows from Lemma 1.3 (iii) that B is a $(|G|/u, u, a, a-m^2, a-m^2+m^2/u)$ semi-regular DDS in G relative to U. The relationship between divisible difference set parameters then fixes $|G| = a^2/(u(a-m^2)+m^2)$. □

If $U = G$ in Lemma 2.1 (so that the BS is covering) then B is equivalent to a $(|G|, a, a-m^2, m^2)$-difference set in G, by Lemma 1.3 (i).

We next show that a BS on a group G relative to a subgroup U can be used to construct a BS on larger groups containing G as a subgroup. In particular we shall construct a semi-regular DDS as a single building block on a group containing G.

Lemma 2.2 *Suppose there exists a (a, m, t) BS on a group G relative to a subgroup U, and let s be an integer dividing t. Then there exists a $(as, m, t/s)$ BS on G' relative to U, where G' is any group containing G as a subgroup of index s.*

Proof Let $\{B_1, B_2, \ldots, B_t\}$ be a (a, m, t) BS on G relative to U.

For each $j = 1, 2, \ldots, t/s$ define the subset $R_j = \cup_{i=1}^{s} g_i' B_{i+(j-1)s}$ of G', where $g_1', g_2', \ldots, g_s' \in G'$ are coset representatives of G in G'. (Although the building blocks B_i can have non-empty intersection, by definition no set R_j contains repeated elements.) Let χ be a non-principal character of G' and consider the character sum $\chi(R_j) = \sum_{i=1}^{s} \chi(g_i')\chi(B_{i+(j-1)s})$. We distinguish three cases.

Case 1: χ is principal on G and non-principal on G' (so $s > 1$). We have $\chi(B_{i+(j-1)s}) = |B_{i+(j-1)s}| = a$ for each ordered pair (i, j), so $\chi(R_j) = a \sum_{i=1}^{s} \chi(g_i') = 0$ for each j. The last equality uses the fact that χ induces a non-principal character on G'/G, and the associated character sum over this group is 0.

Case 2: χ is principal on U and non-principal on G. By assumption we have $\chi(B_{i+(j-1)s}) = 0$ for each ordered pair (i, j) and so again $\chi(R_j) = 0$ for each j.

Case 3: χ is non-principal on U. By assumption $|\chi(B_{i+(j-1)s})| = m$ for exactly one ordered pair (i, j) (say (I, J)) and $|\chi(B_{i+(j-1)s})| = 0$ for all other ordered pairs (i, j). Therefore $|\chi(R_J)| = |\chi(g_I')||\chi(B_{I+(J-1)s})| = m$ and $|\chi(R_j)| = 0$ for each $j \neq J$.

The character sums for each of the three cases show that $\{R_1, R_2, \ldots, R_{t/s}\}$ is a $(as, m, t/s)$ BS on G' relative to U. □

Theorem 2.3 *Suppose there exists a (a, m, t) BS on a group G relative to a subgroup U of order u, and let G' be any group containing G as a subgroup of index t. If $U \neq G'$ then there exists a $(a^2t^2/(u(at-m^2)+m^2), u, at, at-m^2, at-m^2+m^2/u)$ semi-regular DDS in G' relative to U.*

Proof Apply Lemma 2.2 with $s = t$ to obtain a $(at, m, 1)$ BS on G' relative to U, and then use Lemma 2.1. □

The special case $m = \sqrt{at}$ of Theorem 2.3 shows that a $(a, \sqrt{at}, t)$ BS gives rise to a $(at, u, at, at/u)$ semi-regular RDS.

For an example involving divisible difference sets with $\lambda_1 \neq 0$, we can express the DDS construction due to Davis [6] and Pott (reported in [6]) as follows. Denote by $\mathrm{EA}(q^d)$ the elementary abelian group of order q^d, where q is a prime power. Regard $G = \mathrm{EA}(q^{d+1})$ as a vector space P of dimension $d+1$ over $\mathrm{GF}(q)$. There are $t+1 = \frac{q^{d+1}-1}{q-1}$ subspaces $H_0, H_1, \ldots, H_t$ of P of dimension d, called hyperplanes. The hyperplanes have the crucial property that any non-principal character of G is principal on exactly one of the hyperplanes. It follows that $\{H_1, H_2, \ldots, H_t\}$ is a (q^d, q^d, t) BS on G relative to $H_0 \cong \mathrm{EA}(q^d)$. Therefore by Theorem 2.3 there is a $(qt, q^d, q^d t, q^{d-1}(t-q), q^{d-1}t)$ semi-regular DDS in G' relative to U, where G' is any group containing G as a subgroup of index t.

We again follow [7] and introduce a further definition:

Definition For integers $a \geq 0$, $m \geq 1$, and $h \geq 1$, a $(a, m, h, +)$ *extended building set (EBS) on a group G with respect to a subgroup U* is a collection of h building blocks in G with modulus m, of which $h-1$ contain a elements and one contains $a+m$ elements, such that for every non-principal character χ of G:

(i) exactly one building block has nonzero character sum if χ is principal on U;

(ii) each building block has zero character sum if χ is non-principal on U.

We define a $(a, m, h, -)$ EBS on G with respect to U in the same way, with $a+m$ replaced by $a-m$. We can treat both cases simultaneously by referring to a $(a, m, h, \pm)$ EBS. Notice that the role of principal and non-principal characters on U is the reverse of that used in the definition of BS. We call the EBS *covering* in the case $U = \{1_G\}$, when exactly one building block has nonzero character sum for every non-principal character of G.

The next two results are proved in a similar manner to Lemma 2.2 and Theorem 2.3. They show that a covering EBS on a group G can be used to construct a covering EBS on larger groups containing G as a subgroup, and that in particular a difference set can be obtained as a single building block on a group containing G.

Lemma 2.4 *Suppose there exists a $(a, m, h, \pm)$ covering EBS on a group G, and let s be an integer dividing h. Then there exists a $(as, m, h/s, \pm)$ covering EBS on G', where G' is any group containing G as a subgroup of index s.*

Theorem 2.5 *Suppose there exists a $(a, m, h, \pm)$ covering EBS on a group G. Then there exists a $(h|G|, ah \pm m, ah \pm m - m^2, m^2)$-difference set in any group G' containing G as a subgroup of index h.*

All difference sets constructed in this paper will be obtained from covering EBSs by means of Theorem 2.5. We next show that a covering EBS can be "lifted" to form an EBS on a larger group.

Lemma 2.6 *Suppose there exists a $(am, m, h, \pm)$ covering EBS on a group G/U, where U is a subgroup of G of order u. Then there exists a $(uam, um, h, \pm)$ EBS on G with respect to U.*

Proof Let $\{B'_1, B'_2, \ldots, B'_h\}$ be a $(am, m, h, \pm)$ covering EBS on G/U. For each j, let $B_j = \{g \in G \mid gU \in B'_j\}$ be the pre-image of B'_j under the quotient mapping from G to G/U. Since B_j is the union of $|B'_j|$ distinct cosets of U, it follows both that $|B_j| = u|B'_j|$ and that for every non-principal character χ of G:

$$\chi(B_j) = \begin{cases} 0 & \text{if } \chi \text{ is non-principal on } U, \\ u\psi(B'_j) & \text{if } \chi \text{ is principal on } U, \end{cases}$$

where ψ is the non-principal character induced by χ on G/U. By the definition of covering EBS, $\psi(B'_j)$ is nonzero (having modulus m) for exactly one value of j. Therefore $\{B_1, B_2, \ldots, B_h\}$ is a $(uam, um, h, \pm)$ EBS on G with respect to U. □

We are now ready to state the key construction of the paper, which uses a covering EBS on a factor group G/U and a BS on G relative to U to produce a covering EBS on G. By Theorems 2.3 and 2.5, we can view this as using a difference set and a semi-regular divisible difference set to produce another difference set.

Theorem 2.7 *Let G be a group containing a subgroup U of order u. Suppose there exists a $(am, m, h, \pm)$ covering EBS on G/U and there exists a (uam, um, t) BS on G relative to U. Then there exists a $(uam, um, h+t, \pm)$ covering EBS on G.*

Proof By Lemma 2.6 the existence of a $(am, m, h, \pm)$ covering EBS on G/U implies the existence of a $(uam, um, h, \pm)$ EBS, say $\{B_1, B_2, \ldots, B_h\}$, on G with respect to U. By the definition of EBS, a non-principal character χ of G gives a nonzero character sum on exactly one of the building blocks $B_1, B_2, \ldots, B_h$ if χ is principal on U, and gives a zero character sum on all these building blocks otherwise. By assumption there exists a (uam, um, t) BS, say $\{B_{h+1}, B_{h+2}, \ldots, B_{h+t}\}$, on G relative to U. By the definition of BS, a non-principal character χ of G gives a nonzero character sum on exactly one of the building blocks $B_{h+1}, B_{h+2}, \ldots, B_{h+t}$ if χ is non-principal on U, and gives a zero character sum on all these building blocks otherwise. Combining the character properties, we see that the multiset union of the building blocks $\{B_1, B_2, \ldots, B_{h+t}\}$ is a $(uam, um, h+t, \pm)$ covering EBS on G. □

The proof of Theorem 2.7 demonstrates why building sets and extended building sets were introduced. The crucial property, that at most one building block has a nonzero character sum, allows us to combine their favourable character properties simply by taking the multiset union of the constituent building blocks. In the special case $um = at$ of Theorem 2.7, the BS ingredient gives rise to a relative difference set under Theorem 2.3, rather than a divisible difference set with $\lambda_1 \neq 0$.

We can recursively construct covering EBSs using Theorem 2.7, and therefore difference sets by Theorem 2.5, provided the appropriate BSs are available. For this purpose we now state some preliminary lemmas and then give a recursive construction for BSs.

The following lemma, from [7], shows that a BS on G relative to U can be "contracted" by a subgroup W of U to give a BS on the factor group G/W relative to U/W.

Lemma 2.8 *Suppose that $\{B_i\}$ is a $(a, \sqrt{at}, t)$ BS on a group G relative to a subgroup U. Let W be a subgroup of U. Then the images of the $\{B_i\}$ under the quotient mapping from G to G/W form a $(a, \sqrt{at}, t)$ BS on G/W relative to U/W.*

Unlike many of the results developed here from [7], in Lemma 2.8 the condition $m = \sqrt{at}$ on the BS parameters is necessary, so that the contraction of the BS has no repeated elements. (Likewise, the method of contraction is known to apply to RDSs but not to DDSs with $\lambda_1 \neq 0$, for the same reason.)

The next lemma (see [7], for example) describes an important property of hyperplanes.

Lemma 2.9 *Let P be a vector space of dimension 2 over $\mathrm{GF}(p^\alpha)$, where p is prime and $\alpha \geq 1$. Any non-principal character of P is principal on exactly one of the $p^\alpha+1$ hyperplanes of P.*

Corollary 2.10 *Let p be prime and let i, α be positive integers with $i \leq \alpha$. Then there are subgroups $H_0, H_1, \ldots, H_{p^\alpha}$ of $\mathbb{Z}_p^{\alpha+i}$ such that $\{H_1, H_2, \ldots, H_{p^\alpha}\}$ is a $(p^\alpha, p^\alpha, p^\alpha)$ BS on $\mathbb{Z}_p^{\alpha+i}$ relative to $H_0 \cong \mathbb{Z}_p^i$ (where H_0 is contained within exactly i direct factors of $\mathbb{Z}_p^{\alpha+i}$).*

Proof Let $K_0, K_1, \ldots, K_{p^\alpha}$ be the subgroups of $\mathbb{Z}_p^{2\alpha}$ of order p^α corresponding to hyperplanes of P under an isomorphism from $\mathbb{Z}_p^{2\alpha}$ to P. Label the subgroups so that $K_0 \cong \mathbb{Z}_p^\alpha$ is contained in exactly α direct factors of $\mathbb{Z}_p^{2\alpha}$. Then Lemma 2.9 implies that $\{K_1, K_2, \ldots, K_{p^\alpha}\}$ is a $(p^\alpha, p^\alpha, p^\alpha)$ BS on $\mathbb{Z}_p^{2\alpha}$ relative to K_0. This proves the case $i = \alpha$.

For $i < \alpha$, apply Lemma 2.8 with $W \cong \mathbb{Z}_p^{\alpha-i}$ to obtain a $(p^\alpha, p^\alpha, p^\alpha)$ BS on $\mathbb{Z}_p^{\alpha+i}$ relative to $\mathbb{Z}_p^i$ such that each building block of the contracted building set is a subgroup of $\mathbb{Z}_p^{\alpha+i}$. □

We can now give the recursive construction for BSs.

Theorem 2.11 *Let $H_0, H_1, \ldots, H_s$ be subgroups of a group G which are each contained in a subgroup Q of G (the case $Q = G$ being allowed).*

Suppose that $\{H_1, H_2, \ldots, H_s\}$ is a (w, w, s) BS on Q relative to H_0 (when the H_i are viewed as subgroups of Q). Suppose also there exists a (a, m, t) BS on G/H_i relative to Q/H_i for each $i = 1, 2, \ldots, s$. Then there exists a (wa, wm, st) BS on G relative to H_0.

Proof For each $i \geq 1$, let $\{B'_{i1}, B'_{i2}, \ldots, B'_{it}\}$ be a (a, m, t) BS on G/H_i relative to Q/H_i. Following the proof of Lemma 2.6, for each $i \geq 1$ and for each j let $B_{ij} = \{g \in G \mid gH_i \in B'_{ij}\}$. Since B_{ij} is the union of $|B'_{ij}| = a$ distinct cosets of H_i, $|B_{ij}| = wa$, and for every non-principal character χ of G and for each $i \geq 1$ and for each j:

$$\chi(B_{ij}) = \begin{cases} 0 & \text{if } \chi \text{ is non-principal on } H_i, \\ w\psi(B'_{ij}) & \text{if } \chi \text{ is principal on } H_i, \end{cases} \tag{2.1}$$

where $\psi(B'_{ij})$ is the non-principal character induced by χ on G/H_i. By the definition of BS, for each $i \geq 1$, $\psi(B'_{ij})$ is nonzero (having modulus m) for exactly one value of j if ψ is non-principal on Q/H_i, and is zero for each value of j if ψ is principal on Q/H_i.

We claim that $\{B_{ij} \mid 1 \leq i \leq s, 1 \leq j \leq t\}$, comprising st subsets B_{ij} of G, is a (wa, wm, st) BS on G relative to H_0. To establish this, let χ be a non-principal character of G and distinguish three cases.

Case 1: χ is non-principal on Q and on H_0. Since $\{H_1, H_2, \ldots, H_s\}$ is a (w, w, s) BS on Q relative to H_0, we have $|\chi(H_I)| = w$ for some $I \neq 0$ and $\chi(H_i) = 0$ for

each $i \neq I$. But then $|\chi(H_I)| = |H_I|$ (since $|H_I| = w$), so that χ is principal on H_I and non-principal on H_i for each $i \neq I$. Therefore $\chi(B_{ij}) = 0$ for each $i \neq I$ and $\chi(B_{Ij}) = w\psi(B'_{Ij})$, from (2.1). Since χ is non-principal on Q, ψ is non-principal on Q/H_I and so $\psi(B'_{Ij})$ is nonzero (having modulus m) for exactly one value of j. Therefore $\chi(B_{ij})$ is nonzero (having modulus wm) for exactly one ordered pair (i,j).

Case 2: χ is non-principal on Q and principal on H_0. Since $\{H_1, H_2, \ldots, H_s\}$ is a (w,w,s) BS on Q relative to H_0, we now have $\chi(H_i) = 0$ for each $i \neq 0$, so that χ is non-principal on H_i for each $i \neq 0$. Therefore $\chi(B_{ij}) = 0$ for each ordered pair (i,j), from (2.1).

Case 3: χ is principal on Q (note this cannot arise if $Q = G$). In this case χ is principal on H_i for each $i \geq 0$. Therefore $\chi(B_{ij}) = w\psi(B'_{ij})$ for each $i \geq 1$, from (2.1). Since ψ is principal on Q/H_i, $\psi(B'_{ij}) = 0$ for each ordered pair (i,j).

The results for the three cases establish the claim. □

In applying Theorem 2.11 recursively we shall always take the $\{H_i\}$ to be the (q,q,q) BS of Corollary 2.10, derived from the hyperplanes of $\mathrm{EA}(q^2)$ (where $q = p^\alpha$). An alternative direct approach, closer to Chen's original constructions [4], [5], is to make use of the more general $(q^d, q^d, \frac{q^{d+1}-1}{q-1} - 1)$ BS mentioned after Theorem 2.3, based on hyperplanes of $\mathrm{EA}(q^{d+1})$. We believe our recursive method may assist the construction of Chen difference sets in new groups.

3 The McFarland, Spence, Davis-Jedwab and Hadamard Families

In this section we summarise the recursive construction of difference sets in the McFarland, Spence, Davis-Jedwab and Hadamard families from covering EBSs using Theorems 2.7 and 2.11 (see [7] for details). The method will be illustrated in more detail when we discuss the construction of Chen difference sets in Section 4.

Recursive application of Theorem 2.11 yields the following families of BSs. All of the initial BSs needed to begin the recursions can be derived from Corollary 2.10 and Lemma 2.2, with two exceptions: a $(4,2,1)$ BS on $\mathbb{Z}_4^2$ relative to $\mathbb{Z}_2^2$, and a $(8,4,2)$ BS on $\mathbb{Z}_4^2 \times \mathbb{Z}_2 = \langle x,y,z \mid x^4 = y^4 = z^2 = 1\rangle$ relative to $\langle x^2, y^2\rangle \cong \mathbb{Z}_2^2$. These BSs can be obtained from the work of Jungnickel [11], and Arasu and Sehgal [2], respectively.

Theorem 3.1 *For each $d \geq 1$, the following exist:*

(i) A (p^{dr}, p^{dr}, p^{dr}) BS on $\mathbb{Z}_p^{(d+1)r}$ relative to $\mathbb{Z}_p^r$, where p is prime and $r \geq 1$;

(ii) A $(2^{2d+1}, 2^{2d}, 2^{2d-1})$ BS on any group G_d of order 2^{2d+3} and exponent at most 4 relative to a subgroup $U_d \cong \mathbb{Z}_2^2$ contained within two of the largest direct factors of G_d;

(iii) A $(2^{2d+2}, 2^{2d+1}, 2^{2d})$ BS on any group G_d of order 2^{2d+4} and exponent at most 4 relative to a subgroup $U_d \cong \mathbb{Z}_2^2$ contained within two of the largest direct factors of G_d, except possibly $G_1 = \mathbb{Z}_4^3$.

Using Theorem 2.7 and the BSs of Theorem 3.1, we can recursively construct the following families of covering EBSs. The only non-trivial initial covering EBSs required, for case (iii), are equivalent to well-known $(16, 6, 2, 4)$-difference sets.

Theorem 3.2 *For each $d \geq 0$, the following exist:*

(i) *A $(p^{dr}, p^{dr}, \frac{p^{(d+1)r}-1}{p^r-1}+1, -)$ covering EBS on $\mathbb{Z}_p^{(d+1)r}$, where p is prime and $r \geq 1$;*

(ii) *A $(2^{2d+1}, 2^{2d}, \frac{2^{2d+1}+1}{3}, -)$ covering EBS on any group of order 2^{2d+3} and exponent at most 4;*

(iii) *A $(3^d, 3^d, \frac{3^{d+1}-1}{2}, +)$ covering EBS on $\mathbb{Z}_3^{d+1}$;*

(iv) *A $(2^{2d+2}, 2^{2d+1}, \frac{2^{2d+2}-1}{3}, +)$ covering EBS on any group of order 2^{2d+4} and exponent at most 4, except possibly $\mathbb{Z}_4^3$ in the case $d = 1$.*

By applying Theorem 2.5 to the covering EBSs of Theorem 3.2, we deduce the existence of the following families of difference sets.

Corollary 3.3 *For each $d \geq 0$, the following exist:*

(i) *A McFarland difference set with $q = p^r$ in any group of order $q^{d+1}(\frac{q^{d+1}-1}{q-1}+1)$ containing a subgroup isomorphic to $\mathbb{Z}_p^{(d+1)r}$, where p is prime and $r \geq 1$;*

(ii) *A McFarland difference set with $q = 4$ in any group of order $2^{2d+3}(\frac{2^{2d+1}+1}{3})$ containing a subgroup of order 2^{2d+3} and exponent at most 4;*

(iii) *A Spence difference set in any group of order $3^{d+1}(\frac{3^{d+1}-1}{2})$ containing a subgroup isomorphic to $\mathbb{Z}_3^{d+1}$;*

(iv) *A Davis-Jedwab difference set in any group of order $2^{2d+4}(\frac{2^{2d+2}-1}{3})$ containing a subgroup of order 2^{2d+4} and exponent at most 4, except possibly when the subgroup is $\mathbb{Z}_4^3$ in the case $d = 1$.*

Schmidt [21] has recently proved the following exponent bound. Note that for w a positive integer and p prime, we call p *self-conjugate modulo w* if $p^i \equiv -1 \pmod{w_p}$ for some integer i, where w_p is the largest divisor of w coprime to p.

Theorem 3.4 *The Sylow 2-subgroup of a group containing a Davis-Jedwab difference set with $d \geq 1$ has exponent at most 4 provided that 2 is self-conjugate modulo the group exponent.*

Together with Corollary 3.3 (iv), the bound of Theorem 3.4 gives a necessary and sufficient condition for the existence of Davis-Jedwab difference sets, provided that 2 is self-conjugate modulo the group exponent, with the possible exception of the group $\mathbb{Z}_4^3 \times \mathbb{Z}_5$.

The key initial object required for the recursive construction of Hadamard difference sets is a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on a group of odd order m^2. The following examples are currently known.

Theorem 3.5 *There exists a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on the following groups M of order m^2:*

(i) M is the trivial group;

(ii) $M = \mathbb{Z}_{3^\alpha}^2$, where $\alpha \geq 1$;

(iii) $M = \mathbb{Z}_p^4$, where p is an odd prime.

Case (i) of Theorem 3.5 is trivial, but the other two cases are definitely not!

Case (ii) is due to Arasu, Davis, Jedwab and Sehgal [1]. Case (iii) is due to Chen [4], who built on a succession of papers by Xia [25], Xiang and Chen [26], van Eupen and Tonchev [10], and Wilson and Xiang [24].

The following result, based on a construction of Turyn [23], allows us to compose the $(m(\frac{m-1}{2}), m, 4, +)$ covering EBSs of Theorem 3.5 to produce examples in more general groups.

Theorem 3.6 *Suppose there is a $(m_i(\frac{m_i-1}{2}), m_i, 4, +)$ covering EBS on a group M_i of odd order m_i^2 for $i = 1, 2$. Then there exists a $(m_1 m_2(\frac{m_1 m_2 - 1}{2}), m_1 m_2, 4, +)$ covering EBS on $M_1 \times M_2$.*

We can use the covering EBSs described above to find appropriate initial BSs and covering EBSs. Recursive application of Theorems 2.7 and 2.11, followed by Theorem 2.5, leads us to the following conclusion. We write $\prod_i \mathbb{Z}_{a_i}$ to denote the direct product of finitely many groups $\mathbb{Z}_{a_1}, \mathbb{Z}_{a_2}, \ldots, \mathbb{Z}_{a_r}$ for some $r \geq 0$, with the convention that in the case $r = 0$ this represents the trivial group.

Corollary 3.7 *Let M be the group $\prod_i \mathbb{Z}_{3^{\alpha_i}}^2 \times \prod_j \mathbb{Z}_{p_j}^4$, where each $\alpha_i \geq 1$ and where each p_j is an odd prime, and let $|M| = m^2$. Then the following exist:*

(i) A $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on M;

(ii) A $(2^{2d-1}m^2, 2^d m, 2)$ BS on $G_d \times M$ relative to any subgroup of order 2, where $d \geq 1$ and G_d is any group of order 2^{2d} and exponent at most 2^d;

(iii) *A* $(2^{2d-1}m^2, 2^d m, 4, -)$ *covering EBS on* $G_d \times M$, *where* $d \geq 1$ *and* G_d *is any group of order* 2^{2d} *and exponent at most* 2^d;

(iv) *A Hadamard difference set with* $N = 2^d m$ *in* $G_d \times M$, *where* $d \geq 0$ *and* G_d *is any group of order* 2^{2d+2} *and exponent at most* 2^{d+2}.

In [7] it was noted that the special case $m = \sqrt{at}$ of Theorems 2.7 and 2.11 necessarily leads to difference sets with parameters from the McFarland, Spence, Davis-Jedwab or Hadamard family via Theorem 2.5, assuming the BSs are defined on p-groups. The conclusion drawn in [7] was that new parameter families of difference sets might be constructed via these theorems by finding new $(a, \sqrt{at}, t)$ BSs on groups whose order is not a prime power. Such BSs were indeed found by Davis, Jedwab and Mowbray [9], although they do not appear to lead to new difference sets. On the other hand, by removing the condition $m = \sqrt{at}$ from Theorems 2.7 and 2.11 we can obtain the new Chen parameter family, as we now show.

4 The Chen Family

In this section we illustrate the use of the recursive method in detail by constructing Chen difference sets. We begin by recursively constructing an infinite family of BSs. The initial BS is obtained from a $(m(\frac{m-1}{2}), m, 4, +)$ covering EBS on a group of odd order m^2 (which was also the initial object for the construction of Hadamard difference sets in Section 3).

Theorem 4.1 *For each* $d \geq 0$ *there exists a* $(q^{2d+1}(\frac{q-1}{2}), q^{2d+1}, 4q^{2d})$ *BS on* $\mathrm{EA}(q^{2d+2})$ *relative to* $\mathrm{EA}(q^2)$, *where* $q = 3^r$ *or* $q = p^{2r}$ *for* p *an odd prime, and* $r \geq 1$.

Proof The proof is by induction on d. We know from Corollary 3.7 (i) that there exists a $(q(\frac{q-1}{2}), q, 4, +)$ covering EBS $\{B_1, B_2, B_3, B_4\}$ on $\mathrm{EA}(q^2)$, where $|B_1| = q(\frac{q+1}{2})$ and $|B_2| = |B_3| = |B_4| = q(\frac{q-1}{2})$. The key idea of the construction, due to Chen [4], is to note that, by taking the complement of the building block B_1 in $\mathrm{EA}(q^2)$ the character properties of the building set are retained but each building block now has equal size: $\{\overline{B_1}, B_2, B_3, B_4\}$ is a $(q(\frac{q-1}{2}), q, 4)$ covering BS on $\mathrm{EA}(q^2)$. This establishes the case $d = 0$ of the induction.

Now assume the case $d-1$ to be true, thus there exists a $(q^{2d-1}(\frac{q-1}{2}), q^{2d-1}, 4q^{2d-2})$ BS on $\mathrm{EA}(q^{2d})$ relative to $\mathrm{EA}(q^2)$. By Corollary 2.10, with $p^\alpha = q^2$ and $i = \alpha$, there are subgroups $\{H_i\}$ of $\mathrm{EA}(q^4)$ such that $\{H_1, H_2, \ldots, H_{q^2}\}$ is a (q^2, q^2, q^2) BS on $\mathrm{EA}(q^4)$ relative to $H_0 \cong \mathrm{EA}(q^2)$. Apply Theorem 2.11 with $G = \mathrm{EA}(q^{2d+2})$ and $Q \cong \mathrm{EA}(q^4)$ to establish the case d and complete the induction, noting that $G/H_i \cong \mathrm{EA}(q^{2d})$ and $Q/H_i \cong \mathrm{EA}(q^2)$ for each $i \geq 1$. □

We next use Theorem 2.7 and the BSs of Theorem 4.1 to construct recursively an infinite family of covering EBSs. The initial covering EBS is the same as that used in Theorem 4.1.

Theorem 4.2 *For each $d \geq 0$ there exists a $(q^{2d+1}(\frac{q-1}{2}), q^{2d+1}, 4(\frac{q^{2d+2}-1}{q^2-1}), +)$ covering EBS on $\mathrm{EA}(q^{2d+2})$, where $q = 3^r$ or $q = p^{2r}$ for p an odd prime, and $r \geq 1$.*

Proof The proof is by induction on d. There exists a $(q(\frac{q-1}{2}), q, 4, +)$ covering EBS on $\mathrm{EA}(q^2)$ by Corollary 3.7 (i), which gives the case $d = 0$. Assume the case $d-1$ to be true, so that by hypothesis there exists a $(q^{2d-1}(\frac{q-1}{2}), q^{2d-1}, 4(\frac{q^{2d}-1}{q^2-1}), +)$ covering EBS on $\mathrm{EA}(q^{2d})$. We know from Theorem 4.1 that there exists a $(q^{2d+1}(\frac{q-1}{2}), q^{2d+1}, 4q^{2d})$ BS on $\mathrm{EA}(q^{2d+2})$ relative to $\mathrm{EA}(q^2)$. Apply Theorem 2.7 with $G = \mathrm{EA}(q^{2d+2})$, $U \cong \mathrm{EA}(q^2)$ and $a = \frac{q-1}{2}$, $m = q^{2d-1}$, $t = 4q^{2d}$, $h = 4(\frac{q^{2d}-1}{q^2-1})$ to establish the case d. □

By applying Theorem 2.5 to the covering EBSs of Theorem 4.2 we obtain a family of Chen difference sets with q odd.

Corollary 4.3 *For each $d \geq 0$ there exists a Chen difference set with $q = 3^r$ or $q = p^{2r}$ in any group of order $4q^{2d+2}(\frac{q^{2d+2}-1}{q^2-1})$ containing a subgroup isomorphic to $\mathrm{EA}(q^{2d+2})$, where p is an odd prime and $r \geq 1$.*

All of the difference set constructions described in this paper use BSs constructed from Theorem 2.11. Up to this point we have required only the case $i = \alpha$ of Corollary 2.10 to provide suitable subgroups H_i in Theorem 2.11. We will now use the case $i < \alpha$, which will allow us to obtain Chen difference sets with q even. This important idea, of applying contraction before hyperplane lifting, is due to Chen [5]. As before we begin by constructing an infinite family of BSs. The initial BS is obtained from a Hadamard difference set.

Theorem 4.4 *For each $d \geq 1$ there exists a $(q^{2d+1}(q-1), q^{2d+1}, 2q^{2d})$ BS on $\mathrm{EA}(2q^{2d+2})$ relative to $\mathrm{EA}(q^2)$, where $q = 2^r$ and $r \geq 1$.*

Proof The proof is by induction on d. By Corollary 2.10, with $p = 2$, $\alpha = 2r+1$ and $i = 2r$, there are subgroups $\{H_i\}$ of $\mathrm{EA}(2q^4)$ such that $\{H_1, H_2, \ldots, H_{2q^2}\}$ is a $(2q^2, 2q^2, 2q^2)$ BS on $\mathrm{EA}(2q^4)$ relative to $H_0 \cong \mathrm{EA}(q^2)$. By Corollary 3.7 (iv) there exists a Hadamard difference set with $N = q/2$ in $\mathrm{EA}(q^2)$, which by the comment following Lemma 2.1 is equivalent to a $(\frac{q}{2}(q-1), \frac{q}{2}, 1)$ covering BS on $\mathrm{EA}(q^2)$. Apply Theorem 2.11 with $G = Q = \mathrm{EA}(2q^4)$ to obtain a $(q^3(q-1), q^3, 2q^2)$ BS on $\mathrm{EA}(2q^4)$ relative to $\mathrm{EA}(q^2)$, noting that $G/H_i = Q/H_i \cong \mathrm{EA}(q^2)$ for each $i \geq 1$. This establishes the case $d = 1$.

Now assume the case $d-1$ to be true, so that by the inductive hypothesis there exists a $(q^{2d-1}(q-1), q^{2d-1}, 2q^{2d-2})$ BS on $\mathrm{EA}(2q^{2d})$ relative to $\mathrm{EA}(q^2)$. By Corollary 2.10, with $p = 2$ and $i = \alpha = 2r$, there are subgroups $\{H_i\}$ of $\mathrm{EA}(q^4)$ such that $\{H_1, H_2, \ldots, H_{q^2}\}$ is a (q^2, q^2, q^2) BS on $\mathrm{EA}(q^4)$ relative to $H_0 \cong \mathrm{EA}(q^2)$. Apply Theorem 2.11 with $G = \mathrm{EA}(2q^{2d+2})$ and $Q \cong \mathrm{EA}(q^4)$ to establish the case d, noting that $G/H_i \cong \mathrm{EA}(2q^{2d})$ and $Q/H_i \cong \mathrm{EA}(q^2)$ for each $i \geq 1$. □

Note that we have not established whether the case $d = 0$ of Theorem 4.4, namely a $(q(q-1), q, 2)$ BS on $\mathrm{EA}(2q^2)$ relative to $\mathrm{EA}(q^2)$ for $q = 2^r$, exists. However the cases $d \geq 1$ are sufficient to construct recursively an infinite family of covering EBSs. The initial covering EBS is again one of those previously used to construct Hadamard difference sets.

Theorem 4.5 *For each $d \geq 0$ there exists a $(q^{2d+1}(q-1), q^{2d+1}, 2(\frac{q^{2d+2}-1}{q^2-1}), +)$ covering EBS on $\mathrm{EA}(2q^{2d+2})$, where $q = 2^r$ and $r \geq 1$.*

Proof The proof is by induction on d. By Corollary 3.7 (iii) with $m = 1$ there exists a $(q^2/2, q, 4, -)$ covering EBS on $\mathrm{EA}(q^2)$. Apply Lemma 2.4 with $s = 2$ to obtain a $(q^2, q, 2, -)$ covering EBS on $\mathrm{EA}(2q^2)$. This can be equivalently written as a $(q(q-1), q, 2, +)$ covering EBS on $\mathrm{EA}(2q^2)$, which establishes the case $d = 0$.

Now assume the case $d-1$ to be true, so that by the inductive hypothesis there exists a $(q^{2d-1}(q-1), q^{2d-1}, 2(\frac{q^{2d}-1}{q^2-1}), +)$ covering EBS on $\mathrm{EA}(2q^{2d})$. We know from Theorem 4.4 that there exists a $(q^{2d+1}(q-1), q^{2d+1}, 2q^{2d})$ BS on $\mathrm{EA}(2q^{2d+2})$ relative to $\mathrm{EA}(q^2)$. Apply Theorem 2.7 with $G = \mathrm{EA}(2q^{2d+2})$, $U \cong \mathrm{EA}(q^2)$ and $a = q-1$, $m = q^{2d-1}$, $t = 2q^{2d}$, $h = 2(\frac{q^{2d}-1}{q^2-1})$ to establish the case d. □

Finally we apply Theorem 2.5 to the covering EBSs of Theorem 4.5 to obtain a family of Chen difference sets with q a power of 2.

Corollary 4.6 *For each $d \geq 0$ there exists a Chen difference set with $q = 2^r$ in any group of order $4q^{2d+2}(\frac{q^{2d+2}-1}{q^2-1})$ containing a subgroup isomorphic to $\mathrm{EA}(2q^{2d+2})$, where $r \geq 1$.*

In Corollary 4.6, the largest power of 2 dividing the group order is $4q^{2d+2}$, and so the Sylow 2-subgroup of the group containing the Chen difference set is isomorphic to $\mathrm{EA}(4q^{2d+2})$ or $\mathbb{Z}_4 \times \mathrm{EA}(q^{2d+2})$.

Schmidt [21] has recently obtained the following exponent bound for Chen difference sets.

Theorem 4.7 *The Sylow p-subgroup of a group containing a Chen difference set with $q = p^r$ odd, $d \geq 1$ and $r \geq 2$ has exponent at most p^{r-1} provided that p is self-conjugate modulo the group exponent.*

5 Recursive Construction of Building Sets

We have seen that the building sets required for the construction of difference sets in this paper can be obtained recursively from Theorem 2.11. In fact we can obtain many further families of BSs by recursive application of Theorem 2.11, which by Theorem 2.3 gives families of semi-regular relative difference sets or divisible difference sets. In this section we show by means of an extended example how to apply

Theorem 2.11 systematically in this way. The result we obtain occurs as a special case of a more general result proved in [7].

Let p be prime and let G_d be any group of order p^{2dr} and exponent at most p^d containing a subgroup $U_d \cong \mathbb{Z}_p^r$. We wish to find conditions under which there exists a $(p^{(2d-1)r}, p^{dr}, p^r)$ BS on G_d relative to U_d, especially for groups G_d with small rank. We shall recursively apply Theorem 2.11, in each case taking Q to be isomorphic to $\mathbb{Z}_p^{2r}$ and the subgroups $\{H_i\}$ to be the uncontracted hyperplanes of Q (given by the case $i = \alpha$ of Corollary 2.10).

We begin with a (p^r, p^r, p^r) BS on G_1 relative to U_1, which exists by Corollary 2.10. Put $s = p^r$ in Lemma 2.2 to obtain a $(p^{2r}, p^r, 1)$ BS on any group G of order p^{3r}, relative to any subgroup $U \cong \mathbb{Z}_p^r$, subject to the condition: G contains a subgroup S of index p^r and exponent p.

We now wish to apply Theorem 2.11 to obtain a (p^{3r}, p^{2r}, p^r) BS on G_2 relative to U_2. We can do this provided there exists a subgroup $Q_2 \cong \mathbb{Z}_p^{2r}$ of G_2 whose hyperplanes $\{H_i\}$ satisfy the conditions: $H_0 = U_2$ and, for each $i \neq 0$, G_2/H_i contains a subgroup S_2/H_i (containing Q_2/H_i) of index p^r and exponent p. In fact we can show that this condition on each of the factor groups G_2/H_i is implied by the single condition that G_2/U_2 contains a subgroup of index p^r and exponent p, and so:

Proposition 5.1 *There exists a (p^{3r}, p^{2r}, p^r) BS on G_2 relative to U_2 provided G_2/U_2 contains a subgroup of index p^r and exponent p.*

For example, if $G_2 = \mathbb{Z}_p^{2r-2} \times \mathbb{Z}_{p^2}^{r+1}$ (where $r > 1$) and the subgroup $U_2 \cong \mathbb{Z}_p^r$ is written as being contained within r direct factors of G_2 then all choices of U_2 are allowed, except possibly U_2 being contained within the subgroup $\mathbb{Z}_p^{2r-2}$. This demonstrates that the position of the subgroup U_d within G_d is important. In particular, in the case $r = 2$, Proposition 5.1 deals with all groups G_2 and subgroups U_2 except possibly $G_2 \cong U_2 \times \mathbb{Z}_{p^2}^3$.

We now repeat the above procedure. Put $s = p^r$ in Lemma 2.2 to obtain from Proposition 5.1 a $(p^{4r}, p^{2r}, 1)$ BS on any group G of order p^{5r}, relative to any subgroup $U \cong \mathbb{Z}_p^r$, subject to the condition: G contains a subgroup S of index p^r and exponent at most p^2 such that S/U contains a subgroup of index p^r and exponent p.

We next wish to apply Theorem 2.11 to obtain a (p^{5r}, p^{3r}, p^r) BS on G_3 relative to U_3. This can be done provided there exists a subgroup $Q_3 \cong \mathbb{Z}_p^{2r}$ of G_3 whose hyperplanes $\{H_i\}$ satisfy the conditions: $H_0 = U_3$ and, for each $i \neq 0$, G_3/H_i contains a subgroup S_3/H_i (containing Q_3/H_i) of index p^r and exponent at most p^2 such that $(S_3/H_i)/(Q_3/H_i)$ contains a subgroup of index p^r and exponent p. We can likewise show that this condition on each of the G_3/H_i is implied by the condition that G_3/U_3 contains a subgroup of index p^r and exponent at most p^2 and contains a subgroup of index p^{3r} and exponent p, and so:

Proposition 5.2 *There exists a (p^{5r}, p^{3r}, p^r) BS on G_3 relative to U_3 provided G_3/U_3 contains a subgroup of index p^r and exponent at most p^2 and contains a subgroup of index p^{3r} and exponent p.*

This procedure can be repeated, resulting in the following accumulation of conditions on the factor group G_d/U_d.

Theorem 5.3 *Let p be prime. For each $d \geq 1$ there exists a $(p^{(2d-1)r}, p^{dr}, p^r)$ BS on any group G_d of order p^{2dr} and exponent at most p^d relative to any subgroup $U_d \cong \mathbb{Z}_p^r$, where, for $d > 1$, G_d/U_d contains a subgroup of index $p^{(2d-2j-1)r}$ and exponent at most p^j for $j = 1, 2, \ldots, d-1$.*

We note here that the substitution of conditions on the factor groups G_d/H_i by conditions on G_d/U_d, mentioned in the examples above, depends on the following lemma (proved in [7]).

Lemma 5.4 *Let p be prime, let $a \geq 1$ and $d > 1$, and let G be a p-group of order $p^{2dr}a$ and exponent at most p^d containing a subgroup $U \cong \mathbb{Z}_p^r$. Suppose that G/U contains a subgroup of index $p^{(2d-2j-1)r}$ and exponent at most p^j for $j = 1, 2, \ldots, d-1$. Then G contains a subgroup $Q \cong \mathbb{Z}_p^{2r}$ whose hyperplanes $H_0, H_1, \ldots, H_{p^r}$, when viewed as subgroups of G, satisfy the following:*

(i) $H_0 = U$;

(ii) For each $i \neq 0$, G/H_i contains a subgroup S/H_i (containing Q/H_i) of index p^r and exponent at most p^{d-1} such that $(S/H_i)/(Q/H_i)$ contains a subgroup of index $p^{(2d-2j-3)r}$ and exponent at most p^j for $j = 1, 2, \ldots, d-2$.

By inspection, some of the conditions on G_d/U_d in Theorem 5.3 are redundant. In fact it is straightforward to see that the conditions for $j = 1, 2, \ldots, d-2$ are all implied by the condition for $j = d-1$. Therefore we can rewrite Theorem 5.3 as follows.

Corollary 5.5 *Let p be prime. For each $d \geq 1$ there exists a $(p^{(2d-1)r}, p^{dr}, p^r)$ BS on any group G_d of order p^{2dr} and exponent at most p^d relative to any subgroup $U_d \cong \mathbb{Z}_p^r$, where, for $d > 1$, G_d/U_d contains a subgroup of index p^r and exponent at most p^{d-1}.*

For example, take $G_d = \mathbb{Z}_{p^d}^{2r}$ in Corollary 5.5 (so that the condition on G_d/U_d is always satisfied) and let $P(r)$ be the number of partitions of the positive integer r. Then Theorem 2.3 shows that for each $d \geq 1$ and for any prime p there exists a $(p^{2dr}, p^r, p^{2dr}, p^{(2d-1)r})$ semi-regular RDS in $P(r)$ nonisomorphic groups of rank $2r$ relative to any subgroup $\mathbb{Z}_p^r$. Two such groups are $\mathbb{Z}_{p^{d+1}}^r \times \mathbb{Z}_{p^d}^r$ and $\mathbb{Z}_{p^{d+r}} \times \mathbb{Z}_{p^d}^{2r-1}$. This shows that the group rank of the underlying BS, and also of the resulting RDSs, can remain fixed at $2r$ as the group order grows without bound.

For further results similar to Corollary 5.5 we refer the reader to [7].

6 Open Questions

We conclude with some open questions.

1. We have seen that (a, m, t) building sets can be used to construct recursively Chen difference sets. We remark that the construction of Chen difference sets with $q = 2^r$ given in Corollary 4.6, when applied to the case $q = 2$, does not deal with all the groups covered by Corollary 3.3 (iv) even though the parameters then coincide. Does this point to the construction of Chen difference sets in new groups with $q = 2^r > 2$?

2. The construction of Hadamard difference sets in Section 3 for which $n = N^2$ is not a prime power depends on Theorem 3.6. Is there an analogous composition theorem for McFarland difference sets or for Chen difference sets?

3. In view of Theorem 2.3 and some examples given in this paper, can semi-regular divisible difference sets be systematically studied from the point of view of (a, m, t) building sets with $m \neq \sqrt{at}$? Unwieldy parameter sets for DDSs might appear more straightforward in this notation.

References

[1] K.T. Arasu, J.A. Davis, J. Jedwab, and S.K. Sehgal, New constructions of Menon difference sets, *J. Combin. Theory (A)* **64** (1993), 329–336.

[2] K.T. Arasu and S.K. Sehgal, Some new difference sets, *J. Combin. Theory (A)* **69** (1995), 170–172.

[3] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 2nd edition. To appear.

[4] Y.Q. Chen, On the existence of abelian Hadamard difference sets and a new family of difference sets, *Finite Fields and their Applications.* To appear.

[5] Y.Q. Chen, A construction of difference sets. *Designs, Codes and Cryptography.* To appear.

[6] J.A. Davis, Construction of relative difference sets in p-groups, *Discrete Mathematics* **103** (1992), 7–15.

[7] J.A. Davis and J. Jedwab, A unifying construction for difference sets, *J. Combin. Theory (A).* To appear.

[8] J.A. Davis and J. Jedwab, A survey of Hadamard difference sets, *Groups, Difference Sets and the Monster* (ed. K.T. Arasu et al.), de Gruyter, Berlin-New York, 1996.

[9] J.A. Davis, J. Jedwab, and M. Mowbray, New families of semi-regular relative difference sets, *Designs, Codes and Cryptography.* To appear.

[10] M. van Eupen and V.D. Tonchev, Linear codes and the existence of a reversible Hadamard difference set in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5^4$, *J. Combin. Theory (A)* **79** (1997), 161–167.

[11] D. Jungnickel, On automorphism groups of divisible designs, *Canad. J. Math.* **34** (1982), 257–297.

[12] D. Jungnickel, Difference sets, *Contemporary Design Theory: a Collection of Surveys* (ed. J.H. Dinitz and D.R. Stinson), Wiley, New York, 1992.

[13] D. Jungnickel and B. Schmidt, Difference sets: an update, *Geometry, Combinatorial Designs and Related Structures* (ed. J.W.P. Hirschfeld, S.S. Magliveras, and M.J. de Resmini). To appear.

[14] R.G. Kraemer, Proof of a conjecture on Hadamard 2-groups, *J. Combin. Theory (A)* **63** (1993), 1–10.

[15] E.S. Lander, *Symmetric Designs: an Algebraic Approach*, London Mathematical Society Lecture Notes Series 74, Cambridge University Press, Cambridge, 1983.

[16] S.L. Ma and B. Schmidt, A sharp exponent bound for McFarland difference sets with $p = 2$. Preprint (1995), National University of Singapore.

[17] S.L. Ma and B. Schmidt, The structure of the abelian groups containing McFarland difference sets, *J. Combin. Theory (A)* **70** (1995), 313–322.

[18] S.L. Ma and B. Schmidt, Difference sets corresponding to a class of symmetric designs, *Designs, Codes and Cryptography* **10** (1997), 223–236.

[19] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin, 1995.

[20] A. Pott, A survey on relative difference sets, *Groups, Difference Sets and the Monster* (ed. K.T. Arasu et al.), de Gruyter, Berlin-New York, 1996.

[21] B. Schmidt, Nonexistence results on Chen and Davis-Jedwab difference sets. *J. Algebra.* To appear.

[22] R.J. Turyn, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.

[23] R.J. Turyn, A special class of Williamson matrices and difference sets, *J. Combin. Theory (A)* **36** (1984), 111–115.

[24] R.M. Wilson and Q. Xiang, Constructions of Hadamard difference sets, *J. Combin. Theory (A)* **77** (1997), 148–160.

[25] M.-Y. Xia, Some infinite classes of special Williamson matrices and difference sets, *J. Combin. Theory (A)* **61** (1992), 230–242.

[26] Q. Xiang and Y.Q. Chen, On Xia's construction of Hadamard difference sets, *Finite Fields and their Applications* **2** (1996), 87–95.

James A Davis, Department of Mathematics and Computer Science,
University of Richmond, Virginia 23173, USA `jad@newton.urich.edu`

Jonathan Jedwab, Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford, Bristol BS12 6QZ, UK `jij@hplb.hpl.hp.com`

Fred C Holroyd, Kathleen A S Quinn,
Chris Rowley and Bridget S Webb
The Open University
(Editors)

Combinatorial designs and their applications

CHAPMAN & HALL/CRC
Boca Raton London New York Washington, D.C.

Library of Congress Cataloging-in-Publication Data

Combinatorial designs and their applications / editors, Fred C.
Holroyd ... [et al.].
p. cm. (Chapman & Hall/CRC research notes in mathematics
series ; 403)
Includes bibliographical references and index.
ISBN 0-8493-0659-0 (alk. paper)
1. Combinatorial designs and configurations. I. Holroyd, F. C.
(Fred C.) II. Series.
QA166.25.C654 1999
511'.6—dc21 98-51584
CIP

International Standard Book Number 0-8493-0659-0
Printed in the United States of America 1 2 3 4 5 6 7 8 9 0
Printed on acid-free paper